APCO International
Leaders in Public Safety Communications™

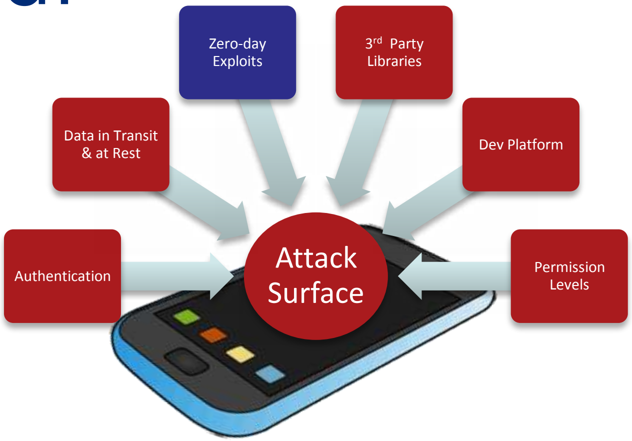
Security and Interoperability of Mobile Applications

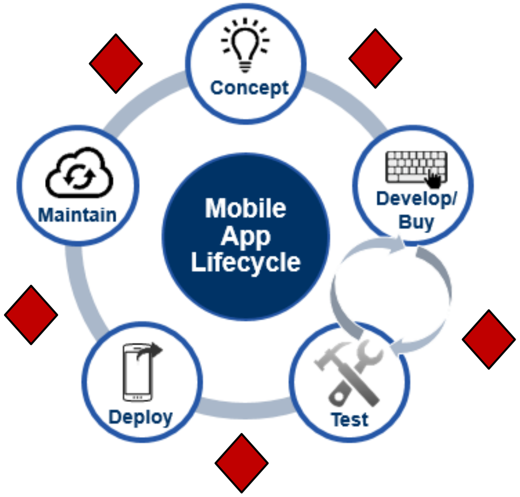
Michael Ogata
PSCR Cybersecurity Project Co-Lead
NIST
michael.ogata@nist.gov

Vincent Sritapan
Mobile Security R&D PM
HSARPA - Cyber Security Division
DHS Science & Technology
dhs.gov/csd-mobile

Mobile Application Security (MAS) Problem: Securing Mobile Apps is Hard!

- Increased use of mobile technologies makes mobile apps the new target for cyber attacks
  - Security state of apps is unknown – may be benign, malicious or potentially unsafe
- Broad and Varied Attack Surface
- Constant Change
  - New apps, app updates, new device OS updates, service provider updates
  - New threats, vulnerabilities, and exploits
- Need Security Assurance – Evaluate Security throughout Mobile App Lifecycle

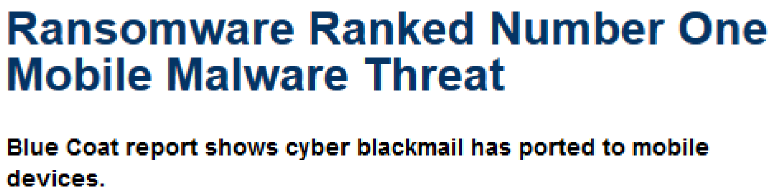




◆ Security Evaluation

Mobile Application Threats

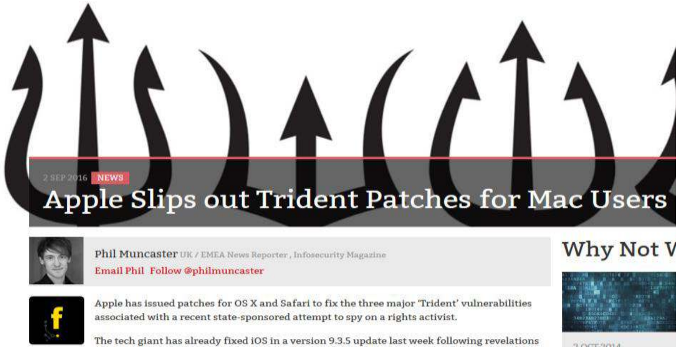
October 2015



Ransomware Ranked Number One Mobile Malware Threat

Blue Coat report shows cyber blackmail has ported to mobile devices.

September 2016



2 SEP 2016 NEWS

Apple Slips out Trident Patches for Mac Users

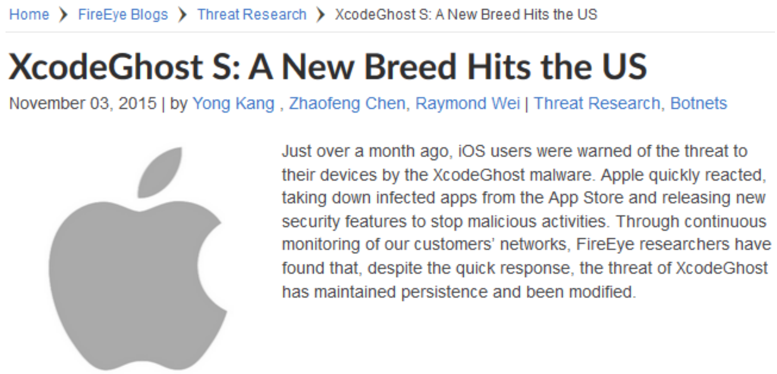
Phil Muncaster UK / EMEA News Reporter , Infosecurity Magazine

Email Phil Follow @philmuncaster

Apple has issued patches for OS X and Safari to fix the three major 'Trident' vulnerabilities associated with a recent state-sponsored attempt to spy on a rights activist.

The tech giant has already fixed iOS in a version 9.3.5 update last week following revelations

November 2015



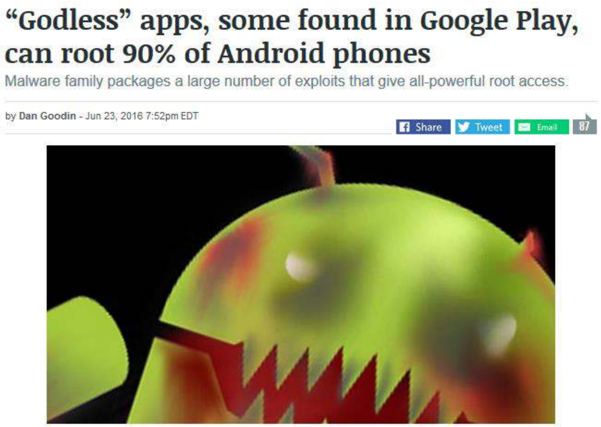
Home ❯ FireEye Blogs ❯ Threat Research ❯ XcodeGhost S: A New Breed Hits the US

XcodeGhost S: A New Breed Hits the US

November 03, 2015 | by Yong Kang , Zhaofeng Chen, Raymond Wei | Threat Research, Botnets

Just over a month ago, iOS users were warned of the threat to their devices by the XcodeGhost malware. Apple quickly reacted, taking down infected apps from the App Store and releasing new security features to stop malicious activities. Through continuous monitoring of our customers' networks, FireEye researchers have found that, despite the quick response, the threat of XcodeGhost has maintained persistence and been modified.

June 2016



"Godless" apps, some found in Google Play, can root 90% of Android phones

Malware family packages a large number of exploits that give all-powerful root access.

by Dan Goodin - Jun 23, 2016 7:52pm EDT

Public Safety Data Type Risk Analysis

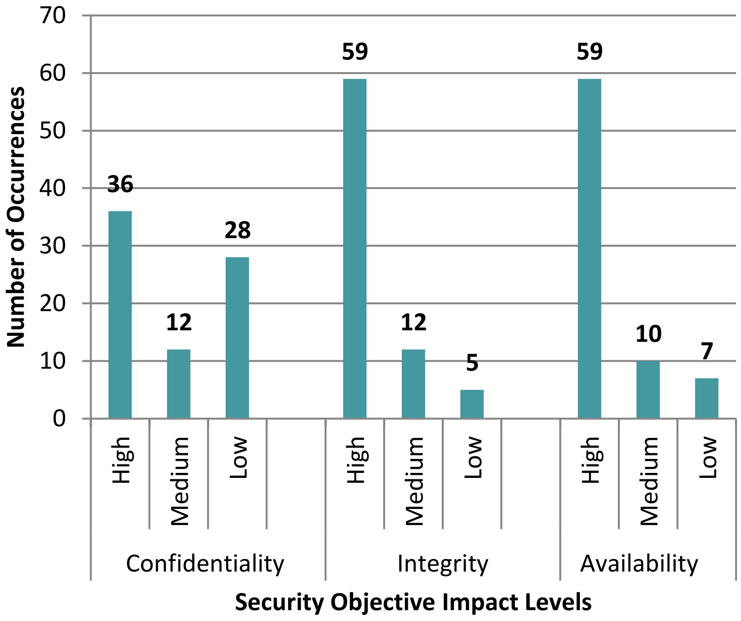
Low

Moderate

High

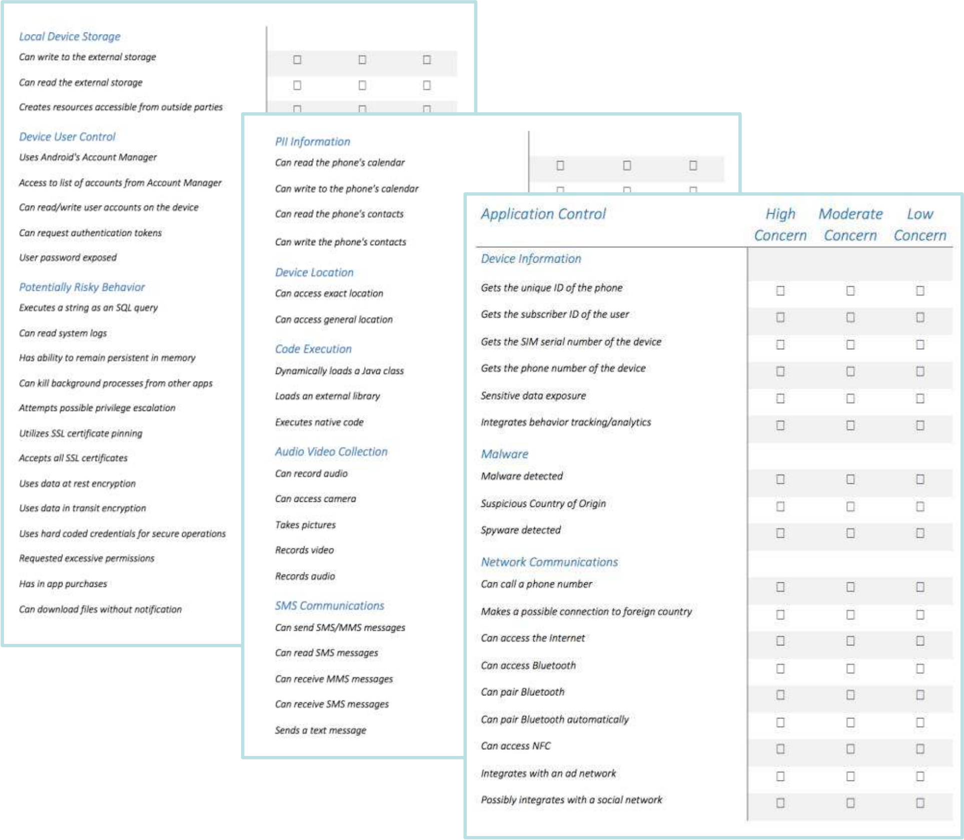
- Mission
- Assets
- Financial Loss
- Harm to Individuals

Identified Data Types	109
Categorized Data Types	76
Uncategorized Data Types	33


Impact Counts Grouped by Security Objective and Impact Level

http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8135.pdf

Mobile App Control List



Local Device Storage			
Can write to the external storage	□	□	□
Can read the external storage	□	□	□
Creates resources accessible from outside parties	□	□	□
Device User Control			
Uses Android's Account Manager			
Access to list of accounts from Account Manager			
Can read/write user accounts on the device			
Can request authentication tokens			
User password exposed			
Potentially Risky Behavior			
Executes a string as an SQL query			
Can read system logs			
Has ability to remain persistent in memory			
Can kill background processes from other apps			
Attempts possible privilege escalation			
Utilizes SSL certificate pinning			
Accepts all SSL certificates			
Uses data at rest encryption			
Uses data in transit encryption			
Uses hard coded credentials for secure operations			
Requested excessive permissions			
Has in app purchases			
Can download files without notification			

PII Information			
Can read the phone's calendar	□	□	□
Can write to the phone's calendar	□	□	□
Can read the phone's contacts			
Can write the phone's contacts			
Device Location			
Can access exact location			
Can access general location			
Code Execution			
Dynamically loads a Java class			
Loads an external library			
Executes native code			
Audio Video Collection			
Can record audio			
Can access camera			
Takes pictures			
Records video			
Records audio			
SMS Communications			
Can send SMS/MMS messages			
Can read SMS messages			
Can receive MMS messages			
Can receive SMS messages			
Sends a text message			

Application Control	*High Concern*	*Moderate Concern*	*Low Concern*
Device Information			
Gets the unique ID of the phone	□	□	□
Gets the subscriber ID of the user	□	□	□
Gets the SIM serial number of the device	□	□	□
Gets the phone number of the device	□	□	□
Sensitive data exposure	□	□	□
Integrates behavior tracking/analytics	□	□	□
Malware			
Malware detected	□	□	□
Suspicious Country of Origin	□	□	□
Spyware detected	□	□	□
Network Communications			
Can call a phone number	□	□	□
Makes a possible connection to foreign country	□	□	□
Can access the Internet	□	□	□
Can access Bluetooth	□	□	□
Can pair Bluetooth	□	□	□
Can pair Bluetooth automatically	□	□	□
Can access NFC	□	□	□
Integrates with an ad network	□	□	□
Possibly integrates with a social network	□	□	□

Take Aways

- Desire for 3rd party solution for app vetting
- App devs are interested in paying for certifications for app security
- App security controls were all relevant to public safety
  - Some controls will be enforced at the jurisdiction level
  - Security perspective varies (mission user, developer, IT enterprise)